

— E-BOOK · THE COMPLETE GUIDE

The Cyber Recovery Handbook.

Why modern ransomware destroys your backups before it encrypts anything, what separates a vault from a backup, and how to build recovery you can actually prove.

12 chapters · 3 frameworks · 6 controls

CONTENTS

What this handbook covers

This guide is for the people who will be in the room during an incident: CISOs and security architects, heads of infrastructure and backup, business-continuity leads, and the executives who will decide whether to pay. It assumes you have backups. The question it answers is whether they will still be there.

01	Why backups stopped being enough Ransomware attacks recovery first	03	02	The six controls that make a vault Immutability, identity, isolation, approval	04
03	Framework 1 — the reachability test Tracing who can actually destroy a copy	05	04	Immutability is a storage property Why policy-based retention is not immutability	06
05	Identity is the real air gap Shared directories and the credential problem	07	06	Clean beats fast Dwell time and infected recovery points	08
07	Framework 2 — the cyber recovery maturity model Five levels from backed up to provably clean	09	08	What belongs in the vault Scoping beyond the obvious systems	10
09	Rehearsing the recovery Why the first real restore should not be the first	11	10	Insurance, audit, and evidence What assessors now ask to see	12
11	Framework 3 — the vault evaluation checklist Twelve questions before you commit	13	12	Getting started Scoping, sizing, and the first exercise	14

THREE FRAMEWORKS YOU CAN REUSE

- **The reachability test** — tracing every path by which a protected copy could be destroyed.
- **The cyber recovery maturity model** — five levels, each defined by what it still cannot prove.
- **The vault evaluation checklist** — twelve questions worth answering before committing.

01 CHAPTER ONE

Why backups stopped being enough

For two decades the answer to ransomware was straightforward: keep good backups, restore, and refuse to pay. That advice was sound, it was widely followed, and attackers read it too.

The modern ransomware sequence — recovery is attacked before production

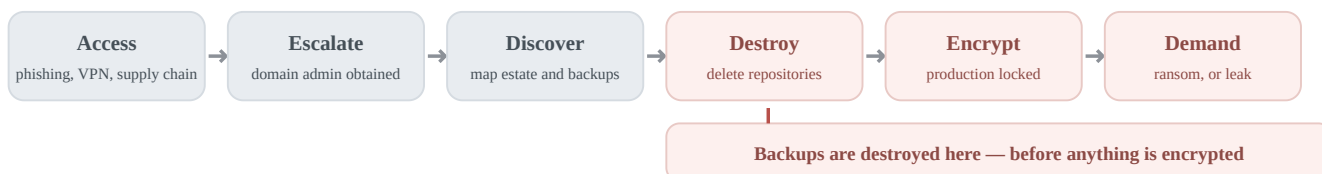


FIGURE 1 — WHERE RECOVERY IS LOST

The sequence above is now standard rather than sophisticated. An intruder who has obtained privileged credentials spends time inside the estate before doing anything visible — enumerating systems, identifying the backup infrastructure, and removing it. Encryption is the last step, not the first, because an organisation that can restore is an organisation that will not pay. By the time the ransom note appears, recovery has usually already been taken away.

Encryption is the ransom note. The attack on your recovery happened quietly, days earlier.

Why good backups fail this test

The backup estates that fail are rarely neglected ones. They fail because they were designed against a different threat: hardware failure, corruption, accidental deletion, site loss. Against those, proximity and convenience are virtues — backups on the network, managed by the same team, authenticated by the same directory, administered through the same console. Against an adversary holding privileged credentials, every one of those virtues is an attack path.

THE DIAGNOSTIC QUESTION

- If someone held your domain administrator credentials for two weeks without being detected, which of your recovery copies would still exist? If the honest answer is "none" or "I am not certain," the rest of this guide is the work.

02 CHAPTER TWO

The six controls that make a vault

"Vault" has become a marketing word attached to anything offsite. The distinction that matters is a specific combination of controls, each of which closes a path the others leave open.

Six controls that make a vault a vault

Storage-layer immutability	WORM objects with retention locks — cannot be altered by any account
Identity isolation	Dedicated vault credentials and RBAC, separate from the production directory
Network isolation	No standing path; connectivity exists only during deliberate transfer windows
Administrative controls	Time-delayed unlock and multi-party approval for destructive operations
Validation	Restorability testing and malware scanning applied to every protected copy
Clean recovery	A separate environment to restore into and verify before returning to production

Remove any one of these and the others can be worked around. A vault is the combination, not any single feature.

FIGURE 2 — THE CONTROL STACK

Why the combination matters

Each control on its own is defeatable. Immutability without identity isolation can be undone by whoever administers the storage. Identity isolation without network isolation still leaves a reachable target. Network isolation without validation gives you an unreachable copy that may not restore. Administrative delay without immutability simply slows a deletion that will still complete.

This is why evaluating a vault by feature list is misleading. The right question is not whether a product offers immutability, but whether the combination leaves any path by which a determined adversary — or a compromised administrator — could remove or corrupt the last clean copy.

A vault is not a feature. It is the absence of a path.

03 FRAMEWORK ONE

The reachability test

The most useful exercise in cyber recovery takes an afternoon and requires no product. For each protected copy, enumerate every way it could be destroyed — then check which of those paths you have actually closed.

THE RULE

- A copy is only protected against an adversary if there is no identity, no network path, and no administrative action that can remove or alter it within its retention window. List all three for every copy you hold.

PATH	QUESTION TO ANSWER	WHAT CLOSING IT LOOKS LIKE
Identity	Which accounts can delete or modify this copy?	Dedicated vault credentials, no trust relationship with production directory
Network	What can reach the storage holding it, and from where?	No standing path; connectivity only during initiated transfer windows
Storage	Can retention be shortened or lifted, and by whom?	WORM enforced at object level, immutable until the lock expires
Administrative	What is the legitimate procedure for destroying data?	Time-delayed unlock with multi-party approval and an audit record
Supply chain	Could the backup software itself be the vector?	Separate credentials and separate control plane from production tooling
Integrity	Could the copy be corrupted rather than deleted?	Validation and malware scanning applied to copies as they land

Running it

Do the exercise with the backup team and the identity team in the same room, because most organisations discover the gap at the seam between them. The backup team knows what the repository permits; the identity team knows which accounts exist and what they can assume. The path that matters is usually visible only when both views are on the same page.

04 CHAPTER FOUR

Immutability is a storage property

Most backup products offer immutability, and most of those offerings would not survive a determined administrator. The difference is which layer enforces it.

Policy versus enforcement

When retention is a setting in the backup application, it is a rule that the application agrees to follow. An account with sufficient rights in that application can change the rule, and an attacker with those credentials will. The protection is real against accident and useless against intent.

Storage-layer immutability — object lock, WORM appliances, retention lock — moves the enforcement beneath the application. The storage refuses the delete or overwrite regardless of what the backup software requests, and regardless of who is asking. The distinction sounds pedantic until the incident, at which point it is the whole difference.

QUESTION	POLICY-BASED RETENTION	STORAGE-LAYER WORM
Who can shorten retention?	Anyone with administrative rights in the backup application	Nobody, until the lock expires
What if the backup server is compromised?	Retention can be changed and copies deleted	The storage still refuses the operation
What if credentials are stolen?	The attacker inherits the ability to disable it	The lock is not a permission that can be assumed
How is it evidenced to an auditor?	A configuration screenshot	A storage-level control with an audit trail

If immutability can be switched off by an account, it is a preference. If it cannot, it is a control.

Choosing a retention window

Retention should exceed your realistic detection time, not your convenient storage budget. Since dwell time is frequently measured in weeks, a seven-day immutable window may lock only copies that already contain the payload. Setting retention against the worst plausible detection delay is what makes a clean recovery point available at all.

05 CHAPTER FIVE

Identity is the **real air gap**

Air gap is usually discussed as a network property. In practice the more important separation is identity, because a shared directory is a path that no firewall rule will close.

Consider the common architecture. Backup repositories sit on the corporate network and authenticate against the production directory, because that is convenient and because it lets the backup team use their normal accounts. The consequence is that a single compromised domain administrator holds both the ability to encrypt production and the ability to destroy the copies intended to recover it. No amount of network segmentation changes that, because the attacker is not crossing the network as an intruder — they are logging in as an authorised user.

Network isolation stops something reaching your vault. Identity isolation stops something being let in.

What identity isolation requires

FOUR PROPERTIES WORTH INSISTING ON

- **No trust relationship** between the vault's identity provider and the production directory.
- **Distinct credentials** that are not stored, cached, or recoverable from production systems.
- **Separate RBAC**, so vault roles are granted independently of production roles.
- **Independent audit**, with vault access recorded where production administrators cannot alter it.

The administrative threat

Identity isolation protects against an external attacker holding stolen credentials. It does not, by itself, protect against the legitimate holder of vault credentials acting maliciously or under coercion. That is what time-delayed unlock and multi-party approval address: making destruction a process with a delay and more than one participant, rather than an action a single authenticated person can complete. For regulated and public-sector estates this is frequently the control that oversight cares about most, because it is the only one that assumes nothing about trust.

Clean beats fast

Having a surviving copy is necessary and not sufficient. The second question — is this copy clean — determines whether recovery ends the incident or restarts it.

The dwell-time problem

An intruder is typically present for a substantial period before detection. Every backup taken during that window may contain the implant, the persistence mechanism, or the staged tooling. Restoring the most recent copy, which is the instinct under pressure, is therefore the action most likely to return the attacker along with the data.

This inverts the usual recovery-point logic. In a conventional disaster the newest copy is the best one. In a cyber incident the newest copy is the most suspect, and the task becomes identifying the most recent point that is demonstrably clean — which is impossible unless something has been checking.

WHAT VALIDATION SHOULD ESTABLISH, PER COPY

- **Restorability** — that the copy actually restores, rather than merely existing.
- **Integrity** — that it has not been corrupted in transit or at rest.
- **Absence of known malicious code** — scanned rather than assumed.
- **Absence of encryption behaviour** — detecting the pattern of an attack already in progress.

Why this belongs in the vault, not beside it

Validation performed on a schedule, automatically, as copies land produces a running answer to the question you will ask under pressure. Validation performed manually during an incident consumes the hours you do not have, with a team that is already fully occupied. The practical value of AI-driven validation is not that machines scan better than people — it is that they scan every copy, continuously, so the answer already exists when it is needed.

In a cyber incident the newest backup is the most suspicious one. Know which point is clean before you need to choose.

07 FRAMEWORK TWO

The cyber recovery maturity model

Each level is defined by what it still cannot prove. Most organisations sit at level one or two and describe themselves at level three.

1	Backed up	Backups exist, run on schedule, and restore individual systems. Cannot prove: that they would survive a compromised administrator.
2	Hardened	Retention policies, restricted consoles, and some form of offsite copy. Cannot prove: that immutability holds when the account enforcing it is compromised.
3	Isolated	Storage-layer WORM, dedicated vault credentials, no standing network path. Cannot prove: that any given copy is free of the payload.
4	Validated	Every copy tested for restorability and scanned for malicious code, with results recorded. Cannot prove: that the full estate recovers in order, within a known time.
5	Rehearsed	Clean recovery exercised end to end with measured times, admin-proof controls, and evidence retained. Cannot prove: nothing material — recovery is demonstrated rather than assumed.

How to use it

The levels are sequential, and the two frequent errors are symmetrical. Validating copies you cannot protect produces confidence in something an attacker can still delete. Protecting copies you never validate produces an unreachable archive that may not restore. The usual stall is between three and four, because isolation is a project with a clear end and validation is an ongoing operational commitment — and ongoing commitments are harder to fund than projects.

A FOUR-QUESTION SELF-ASSESSMENT

- Could a compromised domain administrator delete every copy you hold? **(Level 3)**
- Can you name the most recent recovery point you know to be clean? **(Level 4)**
- How long did your last full clean restore actually take? **(Level 5)**
- Who approves destruction of protected data, and how many people are required? **(Level 5)**

08 CHAPTER EIGHT

What belongs in the vault

Vault capacity costs money, so scope is a real decision. It is usually drawn too narrowly, and always around the wrong axis.

Scope by restart dependency, not by system importance

The instinct is to protect the systems the business considers critical. The better question is which systems are required to restart the critical ones — because recovery fails at the dependency nobody listed. Directory services, certificate authorities, configuration management, licensing servers, and the backup infrastructure's own configuration are rarely on anyone's critical list, and a recovery without them does not complete.

CATEGORY	COMMONLY INCLUDED	COMMONLY MISSED
Core systems	ERP, EHR, core banking, production databases	The configuration that makes them start
Identity	—	Directory services, certificate authorities, secrets
Infrastructure	VM images	Network configuration, DNS, licensing servers
Legacy	—	Long-lived platforms outside the standard backup scope
AI estate	—	Model registries, curated datasets, vector indexes
Operations	—	Runbooks, recovery documentation, contact lists

Recovery does not fail at the system you protected. It fails at the one you did not know it needed.

The AI row deserves particular attention because it is new enough to be absent from most policies. If an application in the top protection tier depends on a model registry or a vector index, those artefacts are in that tier too — regardless of which team owns them or which budget bought the storage they sit on.

09 CHAPTER NINE

Rehearsing the recovery

A recovery procedure that has never been executed is a document, not a capability. The first time an organisation performs a full clean restore should not be during the incident that requires it.

What a real rehearsal surfaces

Organisations that run genuine recovery exercises report a consistent pattern: the failures are almost never in the data. They are in dependency order, credentials that nobody could locate, licensing that refuses to activate in a new environment, DNS and certificate issues, and documentation that assumed knowledge held by one person who was unavailable. None of these appear in a file-level restore test, and all of them extend an incident by days.

EXERCISE TYPE	WHAT IT PROVES	WHAT IT LEAVES UNTESTED
Restore a file	The copy is readable	Everything about bringing a service back
Restore one system	That system can run elsewhere	Dependencies and start order
Tabletop exercise	People understand the plan	Whether the plan is technically correct
Clean-room restore	A validated copy restores into an isolated environment	Cutover back to production
Full rehearsal	The estate recovers, in order, within a measured time	Only behaviour under genuine incident stress

Cadence and evidence

Annual rehearsal proves the procedure worked against an estate that has since changed. Quarterly is materially better, and the practical constraint is usually cost and disruption rather than willingness — which is why rehearsing into an isolated recovery environment, rather than against production, is what makes frequency achievable. The by-product matters too: a dated record of a successful clean restore is precisely the evidence that insurers and auditors now request.

10 CHAPTER TEN

Insurance, audit, and evidence

Cyber insurance has shifted from a financial product to a de facto control framework. Underwriters increasingly require specific backup architecture, and the questions they ask are a reasonable proxy for good practice.

What assessors now ask to see

RECURRING REQUIREMENTS

- **Immutable backups** — object lock or WORM enforcement at the storage layer, not application policy.
- **Credential isolation** — backup credentials separated from the production directory.
- **An isolated copy** — logically or physically separated from the production estate.
- **Recent restore evidence** — a dated, successful restore test within a defined window.
- **Documented procedure** — a recovery runbook that names owners and sequence.

These requirements vary by insurer and policy, and they change. The underlying direction does not: assessors have moved from asking whether backups exist to asking whether they would survive an adversary and whether anyone has checked recently. An organisation that can answer those two questions with records rather than assertions is in a materially better position — on premium, on coverage, and during a claim.

The regulatory overlay

The same evidence serves several regimes at once. Operational resilience requirements in financial services, healthcare data protection obligations, and public-sector assurance frameworks all converge on demonstrable recoverability rather than documented intent. Building the evidence once, as a by-product of regular validated rehearsal, is considerably cheaper than assembling it separately for each assessment.

"We have immutable backups" is a claim. "Here is last quarter's validated clean restore, with timings" is evidence.

11 FRAMEWORK THREE

The vault evaluation checklist

Twelve questions worth putting to any vault, including the arrangement you already have. The signal is whether each answer is a demonstration, a document, or a hope.

- | | |
|--|---|
| ☐ Which accounts can delete or alter a protected copy? | ☐ Is immutability enforced by storage or by application policy? |
| ☐ Does the vault trust the production identity provider in any way? | ☐ Is there a standing network path to the vault storage? |
| ☐ What is the procedure for destroying data, and who must approve it? | ☐ Is there a mandatory delay before destructive operations complete? |
| ☐ Is every copy tested for restorability, and how often? | ☐ Are copies scanned for malicious code before they are needed? |
| ☐ Can you identify the most recent known-clean recovery point? | ☐ Is there an isolated environment to restore into and verify? |
| ☐ When was the last full clean restore, and how long did it take? | ☐ Are directory services, legacy platforms, and AI artefacts in scope? |

Scoring the answers

Sort responses into three categories. **Demonstrated** means someone can show you the control working or the record of the last test. **Documented** means it exists in a design or a contract. **Assumed** means it is reasoning rather than evidence. A credible position produces demonstrated answers to identity isolation, storage-layer immutability, validation, and the date of the last clean restore. Any assumed answer to those four is the most valuable finding in the exercise, because it is the gap that will decide the outcome of an incident.

Ask for the date of the last clean restore. The answer tells you more than any architecture diagram.

12 CHAPTER TWELVE

Getting started

A cyber recovery programme does not begin with procurement. It begins with knowing what would survive today, which is usually a shorter list than expected.

STEP	WHAT TO DO	WHAT IT PRODUCES
1 • Reachability test	Run Chapter 3's exercise with the backup and identity teams together	The list of paths by which copies could be destroyed
2 • Scope by dependency	Trace what is required to restart critical systems, not just the systems themselves	A scope including identity, configuration, legacy, and AI artefacts
3 • Set retention honestly	Choose a window longer than your realistic detection time	A clean recovery point that will actually exist
4 • Isolate identity first	Separate vault credentials before optimising anything else	Closure of the most commonly exploited path
5 • Validate continuously	Test restorability and scan every copy as it lands	A running answer to "which point is clean"
6 • Rehearse and record	Run a full clean restore and document the timings	The evidence insurers, auditors, and your board want

Where UPC Cyber vault fits

The six controls from Chapter 2 arrive as one service: WORM-enabled object storage with retention locks, a logically segmented recovery domain with no standing path, dedicated vault credentials and RBAC, approval-gated destructive operations, AI-driven validation and threat scanning on every copy, and multi-VM instant recovery into a clean environment. It is available within UPC Protect, standalone for existing United Private Cloud customers, or inside a sovereign perimeter where residency requirements apply.

THE FIVE THINGS WORTH TAKING AWAY

- **Recovery is attacked first.** Encryption is the last step, not the first.
- **Identity is the real air gap.** A shared directory is a path no firewall closes.
- **Immutability belongs in storage.** If an account can switch it off, it is a preference.
- **Clean beats fast.** The newest copy is usually the most suspect one.
- **Rehearsal produces the evidence** that insurers, auditors, and boards now require.

IN CLOSING

The last clean copy

Every ransomware negotiation begins at the same point: the organisation has discovered it cannot restore. Everything that follows — the payment decision, the downtime, the disclosure, the board conversation — flows from that single fact.

Preventing it is not primarily a detection problem, and it is not solved by better backups in the ordinary sense. It requires one copy that lives somewhere the attacker's credentials do not reach, under rules that no account can rewrite, checked often enough that you know it will restore and that it is clean. That is a narrow requirement, and it is achievable — but only if it is designed for deliberately rather than inherited from a backup architecture built for a different threat.

BOTTOM LINE

When attackers delete the backups, encrypt production, and demand payment — Cyber vault is how you recover without paying.

Ready to test **your last clean copy?**

Book a Cyber vault architecture review, or run a ransomware recovery simulation with our team.

UPC Cyber vault

UNITEDLAYER.COM



EMAIL

contact@unitedlayer.com



PHONE

+1-888-853-7733



X

x.com/unitedlayer



LINKEDIN

linkedin.com/company/unitedlayer